SIP Access Control Intercom with Relay

User’s Guide

Getting Started
This step by step guide will help you setup and install your Wahsega Labs access control intercom with integrated relay.

www.wahsega.com
Important Notice

This manual and any examples contained herein are provided “as is” and are subject to change without notice. Wahsega Labs Incorporated reserves the right to make changes to its products without notice and advises its customers to obtain the latest version of relevant information before placing orders and to verify that the information being relied on is current.

No title to or ownership of the hardware, software and designs described in this document or any of its parts, including patents, copyrights and trade secrets, is transferred to customers. Wahsega Labs Incorporated makes no representations or warranties regarding the contents of this document. Information in this document is subject to change without notice and does not represent a commitment on the part of Wahsega Labs Incorporated.

Copyright Notice

© 2016 Wahsega Labs, Inc. All rights reserved

Reproduction, adaptation, or translation of this manual is prohibited without prior written permission of Wahsega Labs Company, except as allowed under the copyright laws.

Trademarks

Wahsega Labs Incorporated and the Wahsega Labs Incorporated logo are trademarks of Wahsega Labs Incorporated, Inc. All other brand and product names are trademarks, service marks, registered trademarks, or registered service marks of their respective companies.
Table of Contents

PREFACE ................................................................................................................................. 1
  Important Notice .................................................................................................................. i
  Copyright Notice .................................................................................................................. i
  Trademarks ........................................................................................................................... i

CHAPTER 1: OVERVIEW ......................................................................................................... 3
  Intercom Functionality ......................................................................................................... 4
  Quality Standards ............................................................................................................... 5

CHAPTER 2: GENERAL HARDWARE INSTALLATION .............................................................. 6
  Request to Exit and Door Latch Wiring ............................................................................... 6
  Auxiliary Output (Door Control) ......................................................................................... 7
  Door Status Monitor & Request to Exit Button .................................................................. 8
  Door Status Monitor & REX Connector ............................................................................. 9
  Software-based Factory Reset ......................................................................................... 10
  Software Capabilities ....................................................................................................... 12

CHAPTER 3: USER EXPERIENCE ............................................................................................ 13
  Getting Started .................................................................................................................. 14

CHAPTER 4: CONFIGURATION AND WEB INTERFACE ....................................................... 17
  Call Settings ....................................................................................................................... 18
  Buttons & Status Lights ..................................................................................................... 20
  Door Control and Monitor .................................................................................................. 23
  Account Settings .............................................................................................................. 27
  Audio Settings ................................................................................................................... 31
  Network Configuration ...................................................................................................... 34
General System Configuration

Firmware Management

APPENDIX A: MAKING PEER-TO-PEER CALLS

Setting Up Account Information

Receiving Peer-to-Peer Calls to an Intercom

Placing Peer-to-Peer Calls from an Intercom

Placing Peer-to-Peer Calls on a SIP Server
Chapter 1
Overview

The Wahsega Labs access control intercom product line offers the highest quality two-way audio and durability in the industry today. Each and every Wahsega Labs product is designed and manufactured in the USA, ensuring a superior product at the best price available in the market.
Intercom Functionality

Wahsega Labs access control intercoms’ initial functionality includes:

SIP phone/intercom
- Crystal clear audio
  - High-definition 16kHz (wideband) and 32kHz (ultra-wideband)
  - Full-duplex (two-way) conversations
  - Acoustic echo cancellation
  - Background noise suppression algorithm
- Extensive interoperability with most SIP servers and PBXs
- Peer-to-peer (P2P) mode for decentralized communication
- Multiple audio codecs, including G.722, G.711, DVI4, Speex, SILK, PCM and iLBC

Door Control and Monitor
- Support for external Request to Exit (REX) button and/or motion exit
- Direct door latch control
  - Internal switch for control of devices up to 24VDC @ 1.5A
  - Included Form C (SPDT) relay rated for 30VDC or 270VAC @ 3A
- Door closed status monitor input

Web-based configuration
- All configuration options accessible via easy-to-use HTTP Web interface

Industrial Temperature Range (-40°C to +85°C)
Conformal coating on products designed for outdoor installations
PoE 802.3af powered
Quality Standards

Wahsega Labs access control intercoms achieve the highest standards of performance in the market by utilizing our complete quality assurance program encompassing software testing, product design and a multistage automated factory test program.

- Wahsega Labs’ ultimate goal is to provide a solution that is both cost effective and unsurpassed in quality. By leveraging existing relationships with suppliers to guarantee premium components at the lowest possible prices, we are able to ensure Wahsega Labs products are the finest quality in the market while still offered at highly competitive prices directly to installers.

- In order to achieve the greatest possible voice clarity, all voice and related algorithms have been individually tested to ensure the highest potential MOS score. The accumulated error syndrome, which can cause poor voice quality, is mitigated through this testing process.

- Wahsega Labs’ engineering team utilizes a wide array of dedicated test servers to pull and build the various software projects multiple times per day. Each automatic build is then run through an extensive set of automated test cases to ensure the highest performance of each and every firmware version released. This test case coverage is expanded on a continual basis.

- All Wahsega Labs products are 100% factory tested at the board level through a bed of nails full functional test, not just an “is it close enough?” flying probe test. Every finished product is 100% tested again after the final assembly via an automated test station to ensure the highest production quality product for installers.

- To assure the highest quality standards, all Wahsega Labs products are designed, developed and manufactured in the USA.
Chapter 2
General Hardware Installation

Request to Exit and Door Latch Wiring

The access control intercom provides connections for controlling magnetic door latches, Request to Exit (REX) functionality for buttons and/or exit motion sensors as well as door status monitor.

Image A

Detail A

Wiring diagram for Wahsega Access Control Intercom with integrated relay
Auxiliary Output (Door Control)

The connector for Auxiliary Output is a 3-pin male connector, wired to a Form C relay (SPDT), used to connect and control door latches, gates and other points of entry. Its contacts are rated for 30VDC or 270VAC at 3A.

- **Pin 3** is Normally Open (NO).
- **Pin 2** is Common (COM).
- **Pin 1** is Normally Closed (NC).
Door Status Monitor & Request to Exit Button

The connector for the Request to Exit button (REX and door status monitor is a 4-pin male connector used to monitor the door open/closed status as well as the REX button/motion sensor functionality.

- **Pin 4**: REX ground reference pin. Connect to Common.

- **Pin 3**: REX button and/or motion activated exit monitor line. Can be wired as a ground/open button or switch. It is pulled up by 4.7k to 3.3V and wired through 220Ω. Connect to the NO of an SPDT connection.  
  
  *NOTE 1*

- **Pin 2**: Door status ground reference pin. Connect to Common.

- **Pin 1**: Door status monitor line. It can be wired as a ground/open button or switch. It is pulled up by 4.7k to 3.3V and wired through 220Ω. Connect to the NO of an SPDT.  
  
  *NOTE 2*

*NOTE 1*: The REX has a detection de-bounce period of 130 milliseconds minimum. Otherwise detection is not guaranteed.

*NOTE 2*: Door status monitor has a detection de-bounce period of 300 milliseconds minimum. Otherwise detection is not guaranteed.
Door Status Monitor & REX Connector

The Request to Exit (REX) input can be wired in parallel with an REX button and a motion sensor. Both REX and door status inputs go to Normally Open (NO) connections on corresponding devices.
Software-based Factory Reset

As a “reset to factory defaults” function, two pins on the Auxiliary I/O Expansion 7-pin connector (labeled “J29” on the top right of the board) can be jumpered together using a standard 2mm electrical jumper. When the access control intercom boots up, it will check to see if these pins are jumpered, and if so, it will perform a “factory reset”. Which pins are jumpered together determines the type of factory reset performed:

- Jumper pins 2 & 3: Erases the info.json file and all settings revert to defaults.
- Jumper pins 3 & 4: Reserved for future use (no current function).
- Jumper pins 4 & 5: Format the file system.

Because this is a software-based reset, the software must be minimally functional in order to use it. In other words, it cannot be used to recover a unit which has been loaded with a firmware image that does not boot.
Steps for activating the factory reset:

1. Unplug the access control intercom from power, and if anything is connected to the 7-pin connector, unplug that as well.

2. Install a 2mm jumper on the two pins according to which type of factory reset you want. (For example, to erase the configuration and revert to default settings, install a jumper across pins 2 and 3.)

3. Plug in power to the access control intercom (using PoE).

4. Wait **at least 10 seconds** for the access control intercom to boot, read the jumper, and apply the factory reset.

5. Unplug the access control intercom from power.

6. Remove the jumper.

7. Reattach any cables or devices that you detached. When the access control intercom boots up, it will have been restored to factory defaults based on the jumpers.
Software Capabilities

The access control intercom’s main user interface, accessible through the front panel, consists of one button and a bi-color LED (green & red).

To operate, simply press the “call” button, which places a SIP call to a configured phone number or extension. When a recipient answers, they can speak to the caller and enter a DTMF code to unlock the door.

A second button or input can be located remotely from the access control intercom and used as a “Request to Exit” button and/or motion sensor to unlock the door from inside. Alternately, a second call button can be installed and used to dial a different number or extension.

The access control intercom can also be configured to accept incoming calls from authorized users to perform administrative functions.

Touch-Tone DTMF codes can be used for controlling the door lock (for instance, setting it to remain unlocked). These codes are normally kept secret and only used by administrators or maintenance personnel.

If a door closed sensor is installed, a “door ajar” alarm can be configured to place a call to a specified number or extension to alert the recipient. The door closed sensor can also be used to shorten the period of time that the door was left momentarily unlocked.

The access control intercom’s configuration is accessible using an HTTP Web interface, viewable from any Web browser on the same LAN. This allows access to various settings such as network/IP address and SIP account configuration, intercom/call box and door lock behavior, and administrative functions such as firmware upgrade and configuration backup/restore. The configuration is stored in a .JSON file, which is human readable and can be edited by site administrators.
Follow these basic instructions for getting started with the access control intercom.
Getting Started

1. Connect the SIP access control intercom’s Ethernet port to a network using a Power-over-Ethernet (PoE) Ethernet connection. When connected, it will power on immediately and make an audible “beep.”

2. Locate and note your SIP access control intercom’s MAC address. It is printed on a white sticker on the rear of the circuit board, near the Ethernet port and under the speaker.

3. Discover the SIP access control intercom’s IP address. When it boots, it uses DHCP by default to automatically obtain a suitable IP address on your local area network (LAN). It also runs Simple Service Discovery Protocol (SSDP) so you can discover it from Windows Explorer or any SSDP-enabled application.

   From a Windows PC on the same LAN, open “My Computer.” In the left-hand pane, go to the “Network” view.

   Right-click in the right-hand Network pane and select “Refresh.” This will start a search for devices on the network. You may get a popup asking if you want to allow your PC to search the network, in which case you should click “yes” or “allow.”

   If you are not using SSDP or cannot discover the access control intercom on your network, you can:

   - consult your DHCP server’s logs to determine its IP address;
   - use a network discovery app (such as Fing on iOS and Android);
   - or
   - use Wireshark to observe the DHCP network traffic.
4. Once the search is complete, the access control intercom will appear in the Network view as “Wahsega AC Intercom (:XX:XX).” The last two octets of its MAC address will be included in its name, so you can easily distinguish multiple units. Double-click the intercom’s icon to open its Web interface.

5. After you determine the SIP access control intercom’s IP address, navigate to that IP address in your Web browser (for example, http://123.456.78.9).

6. When you access the webpages, the SIP access control intercom will ask for a username and password. The default username and password are “admin” and “admin”.

7. On the right side of the page is the Status bar. It shows the current status of the door lock and sensor, the SIP account status (default status is unconfigured and unregistered), and the access control intercom’s system information (current IP address, Ethernet MAC address and system time).
8. To change the IP address settings, go to the Network page and modify settings in the WAN section. To set the network for DHCP, click the Dynamic IP radio button. For static IP addressing, click the Static IP radio button and fill in the relevant IP address fields with values from your network administrator.

9. To change the SIP account settings, go to the Accounts page and modify settings in the account. Most users will only need to set Username/Number (the phone number or extension assigned to this access control intercom) and Domain (the hostname or IP address of your SIP server). You may also provide an Account Name, which is used only for logging purposes, and a Display Name, which may be used by your SIP server depending on its configuration.

If a password is required for your SIP server or proxy server, provide it in the Password field. If your SIP server or proxy server requires an authentication username that is different from the name entered in Username/Number, enter it on the account’s Advanced tab in the Auth Username field.

10. After configuring the network and SIP settings for your access control intercom, use the configuration settings described in the next sections to customize the intercom/call box and door lock functionality.
The Web interface is a set of webpages used to configure the various settings available on the access control intercom. It allows the access control intercom to be configured from any computer or device with a Web browser.
Call Settings

The Calls page configures settings for outbound and inbound calls.

**Outbound Calls**

- **Ringback tone** – The sound to be played when an outbound call is ringing. Default is the standard “ringing” noise, or administrators can upload a custom file to use. **NOTE 3**

- **Outbound ring limit** – How long to attempt an outbound call before giving up as “not answered.” **Caution: If you select “no limit” but do not have a button configured to hang up calls being attempted, it may be possible for the phone to ring forever if a call is not answered.”
Inbound Calls

- Allow inbound calls – If checked, inbound calls are allowed according to the **Inbound ring limit** (below). If unchecked, inbound calls are immediately rejected.

- Inbound ring limit – If set to “Answer immediately,” inbound calls are immediately answered by the access control intercom, with no rings. If set to “(x) ring(s),” inbound calls ring for that duration. While an incoming call is ringing, pressing the primary button/input will answer that call. If the call is not answered within the inbound ring limit, the call is rejected.

---

*NOTE 3:* Uploaded files must be of WAV type, uncompressed PCM audio, encoded at 16-bit mono, with a sample rate of 8, 16, 32, or 48 kHz. There is file size limit of 900KB; this gives you just under 1 minute of audio at 8 kHz or just under 30 seconds of audio at 16 kHz. This limit is shared between all uploaded audio files on the system.
The *Buttons/Lights* page configures settings for all buttons and lights.
Buttons

- **Primary button/input** – Settings for the main button on the front of the intercom.
  - Phone number – The number or extension to call when the primary button is pressed.
  - Repeat function – What to do when the primary button is pressed while a call is in progress.
  - Inbound calls – If the primary button is configured to hang up calls (*Repeat function*, above), this setting enables it to function on inbound calls in addition to outbound calls. *When an inbound call is set to ring, pressing the button always answers the call. This setting determines whether or not the button can hang up that call, as well.*

- **Secondary button/input** – This may be an external Request to Exit button (REX) or exit/motion sensor OR a second button on the front of the intercom.
  - Installed – Whether or not a secondary button or input is attached to the system.
  - Function – What the second button/input does when triggered: Place a call, trigger a momentary unlock or send a DTMF key sequence while a call is in progress.
  - Phone Number – If the secondary button/input is configured to make a call, this is the number or extension dialed when the secondary button is pressed.
  - Repeat function – If the secondary button is configured to make a call, this is what will happen when the button is pressed while a call is in progress.
  - Inbound calls – If the secondary button is configured to both make and hang up calls, this setting enables it to hang up on inbound calls in addition to outbound calls.
Status Lights

- Selects the condition in which the LED will be lit green or red, steady (“lit”) or blinking.
- The LED may appear in the given state under the following circumstances:
  - Unused / not present – This LED state is never used.
  - When call is in progress (off-hook) – The LED will be lit in this fashion when the call is initiated (ringing) but not yet answered.
  - When call is successful – The LED will be lit in this state when the call has been answered and is connected.
  - When call is in progress and successful – The LED will be lit in this state while the call is being initiated (ringing) and while the call is successfully connected once answered.
# Door Control and Monitor

**Door Lock Settings**
- **Door lock**: Installed
- **Lock type**: Apply power to open lock (fall secure/ fail locked)

## Door Controls
- **Momemtary unlock code**: 123
- **Unlock duration**: 3 seconds
- **Play tone on "momentary unlock" code entry**: Enable
- **Hang up after "momentary unlock" code entry**: Enable
- **Allow leaving door unlocked**: Enable
- **Leave door unlocked code**: 535
- **Leave door locked code**: 534
- **Play tone on "Leave door locked/unlocked" code entry**: Enable
- **Hang up after "Leave door locked/unlocked" code entry**: Enable

**Request To Exit (REX)**
To configure a Request To Exit button or a motion sensor, go to the **Buttons/Lights** page and enable SecondBody button/input pair with the function "Unlock door from inside."

## Door Position Sensor
- **Door position sensor**: Installed
- **Sensor type**: Circuit closes when door is closed (normally open)
- **Finish momentary unlock early when door is opened**: Enable

## Door Ajar Alarm
- **Door ajar alarm**: Enable
- **Alarm period**: 10 minutes
- **Phone number to dial**: Enter
- **Alarm message**: Pay

To upload a new alarm message, drag a .wav audio file here, or click to choose a file.
- **Repeat alarm every**: 15 minutes
The *Door* page configures settings for the door lock and door sensor.

**Door Lock Settings**
- Door lock installed – Whether or not a door lock is attached to the intercom.
- Lock type – Indicates whether sending power to the lock causes it to latch or unlatch.

**Door Controls**
- Momentary unlock code – The Touch-Tone DTMF sequence to enter during a call to trigger a momentary unlock.
- Unlock duration – How long a momentary unlock lasts.
- Play tone on “Momentary unlock” code entry – Enables or disables a notification tone to let the access control intercom user know the momentary unlock code was entered successfully.
- Hang up after “Momentary unlock” code entry – If selected, the call will automatically be ended after a momentary unlock is triggered.
- Allow leaving door unlocked – Enables a separate set of codes to leave the door unlocked continuously. (This is not suitable for some types of locks, such as ones that operate on direct AC power.)
- Leave door unlocked code – The DTMF sequence to enter during a call to leave the door unlocked. This code can be used from any phone, so it should be reasonably long and kept secret except for intended users.
- Leave door locked code – The DTMF sequence to enter during a call to return the door to its normal locked state, with momentary unlocking allowed.
• Play tone on “Leave door locked/unlocked” code entry – Enables or disables a notification tone to let the user know the “Leave door locked/unlocked” code was entered successfully.

• Hang up after “Leave door locked/unlocked” code entry – If selected, the call will automatically be ended after a “Leave door locked/unlocked” code is entered.

Request to Exit (REX)

• To configure a request to exit button or a motion sensor, go to the Buttons/Lights page and enable Secondary button/input with the function "Unlock door from inside."

Door Position Sensor

• Door position sensor installed – Whether or not a door position (open or closed) sensor is installed.

• Sensor type – Indicates whether the sensor closes its circuit when the door is open or closes its circuit when the door is closed.

• Finish momentary unlock early when door is opened – If selected, when a momentary unlock is triggered and the door is subsequently opened, the momentary unlock will finish even though the time limit has not been reached.

Door Ajar Alarm

• Door ajar alarm – Enables an alarm if the door is left open for a prolonged period of time.

• Alarm period – How long the door must remain open before first triggering the alarm.

• Phone number to dial – The number or extension the device calls with the alarm message.
- Alarm message – The sound to play during an alarm. The default is a siren, or the administrator can upload and use a custom audio file. See Note 3 on page 19 for custom file specifications.

- Repeat alarm every – After the first alarm phone call, additional calls will be made at this interval until the door is closed.
Account Settings

The *Accounts* page configures settings for SIP accounts and RTP multicast audio streaming.
**SIP Account**

- This device’s SIP account settings
  - **Use SIP server** – If this box is checked, the account must register with a server to send or receive calls. If unchecked, the account will operate in peer-to-peer (P2P) mode. See [Appendix A](#) for more information regarding P2P calls.
  - **Account name** – The name to use to identify this account. It will only be shown on this page and in the system logs.
  - **Display name** – The name to report to the SIP server, which may be shown to other callers (depending on the SIP server's configuration).
  - **Username/Number** – The phone number or extension this phone is configured with on the SIP server.
  - **Domain** – The hostname or domain name of the SIP server. Not used in P2P mode.
  - **Register with domain** – If checked, operates in normal SIP mode. If unchecked, operates in peer-to-peer (P2P) mode.
  - **Password** – If the SIP server requires a password to authenticate, enter it here.
  - **Topology, QoS, Advanced** – Additional SIP settings accessible after clicking green “Showing Basic Settings” button at the top of the webpage.

**RTP Multicast high priority**

- Stream audio via your access control intercom, using RTP multicast streaming. *Multicast streams on this IP address will take priority over all other transmissions, including SIP calls.*
  - **Account name** – The name to use to identify this account. It will only be shown on this page and in the system logs.
- **Multicast IP address** – The multicast IP address this device should “listen on” to receive RTP audio.
  - Valid addresses range from **224.0.0.1** to **239.255.255.255**.
  - *Some addresses, particularly in the 224.xx.xx.xx range, are globally reserved and should not be used! Consider using addresses in the 239.255.xx.xx range, which are “Administratively Scoped Local Addresses.”*

- **Port** – The UDP port this device should “listen on” to receive RTP audio.
  - Valid ports range from **1** to **65535**. Setting this to **0** will use the default port, which is **5004**.
  - Recommended values are **49152–65535**, but any port that isn’t already in use by the system can be chosen.

**RTP Multicast low priority**

- **Stream audio via your access control intercom, using RTP multicast streaming.** Multicast streams on this IP address will take priority over “background priority” RTP multicast audio streams but will not take priority over SIP calls.

- **Account name** – The name to use to identify this account. It will only be shown on this page and in the system logs.

- **Multicast IP address** – The multicast IP address this device should “listen on” to receive RTP audio.
  - Valid addresses range from **224.0.0.1** to **239.255.255.255**.
  - *Some addresses, particularly in the 224.xx.xx.xx range, are globally reserved and should not be used! Consider using addresses in the 239.255.xx.xx range, which are*
“Administratively Scoped Local Addresses.”

- Port – The UDP port this device should “listen on” to receive RTP audio.
  - Valid ports range from 1 to 65535. Setting this to 0 will use the default port, which is 5004.
  - Recommended values are 49152–65535, but any port that isn’t already in use by the system can be chosen.

**RTP Multicast background priority**

- Stream audio via your access control intercom, using RTP multicast streaming. Multicast streams on this IP address will not take priority over any other transmissions.

- Account name – The name to use to identify this account. It will only be shown on this page and in the system logs.

- Multicast IP address – The multicast IP address this device should “listen on” to receive RTP audio.
  - Valid addresses range from 224.0.0.1 to 239.255.255.255.
  - Some addresses, particularly in the 224.xx.xx.xx range, are globally reserved and should not be used! Consider using addresses in the 239.255.xx.xx range, which are “Administratively Scoped Local Addresses.”

- Port – The UDP port this device should “listen on” to receive RTP audio.
  - Valid ports range from 1 to 65535. Setting this to 0 will use the default port, which is 5004.
  - Recommended values are 49152–65535, but any port that isn’t already in use by the system can be chosen.
The *Audio* page configures settings for audio and codec.
Intercom Audio

- Speaker volume – The default speaker volume setting is 6, with 1 as the softest and 9 as the loudest. Also allows muting the speaker. *Volumes above 7 use digital software gain and may reduce audio quality.*

- Microphone volume – The default volume setting volume of the microphone is 6, with 1 as the softest and 9 as the loudest. Also allows muting the microphone. *Volumes above 6 use digital software gain and may reduce audio quality.*

- Microphone high-pass filter – Eliminates low-frequency noise which can make speech difficult to understand.
  - DC blocker – Only eliminates hum from power lines while leaving other low-frequency sounds intact.
  - High-pass mode – Eliminates most noise below standard telephone frequencies.

- Advanced settings – Accessible upon clicking green “Showing Basic Settings” button at the top of the webpage.
  - Microphone boost – Enables the microphone boost, which adds +20dB of hardware gain. *This should normally be left enabled,* but some microphones may sound better with it disabled.
  - Echo canceller – Reduces echo caused by feedback from the speaker to the microphone. It has no effect locally at the intercom itself; it is only audible to the party on the other end of a call.
  - Noise reduction – This option reduces background noise such as fans and hums. It has no effect locally at the intercom itself; it is only audible to the party on the other end of a call.
Codec Selection

- Choose preferred codecs – These settings enable/disable audio codecs and set their order of use. The system tries codecs at the top of the Preferred list before trying codecs at the bottom of the list.
The *Network* page configures settings for TCP/IP networking.
WAN

- General Network Settings
  - Host – Enter your network’s hostname. (*May be empty.*)
  - Domain – Enter your network’s domain name. (*May be empty.*)
- Connection Type
  - Dynamic IP – Choose this to use DHCP to assign an address automatically. Note that when using DHCP, you will have to determine the IP address assigned to the access control intercom using your DHCP server or through some other method in order to access the configuration webpages in the future.
  - Static IP – Choose this to enter IP address settings manually.
    Warning: If you enter a configuration that is not accessible from your network, you may be unable to communicate with the access control intercom! Double-check that the settings you enter are correct before rebooting the intercom to apply them.
    - Be sure to include address, mask, default router and DNS primary. Some networks require a secondary and/or tertiary DNS as well.
- Advanced settings – Access by clicking green “Showing Basic Settings button at the top of the webpage.
  - Enable IGMPv3 (advanced) – Check to enable IGMP version 3 on your speaker. If unchecked, IGMP version 2 (IGMPv2) will be used. Default setting is disabled. If you know that your routers have IGMPv3 enabled, you can safely enable this setting. *If unsure, leave disabled* to ensure support with routers that only use IGMPv2.
- MTU size (advanced) – Maximum transmission unit allowed on the Ethernet connection. The standard for Ethernet networks is 1500, and you should not change this value unless directed by your network administrator.

- Force slower 10Mbps link speed (advanced) – Forces the Ethernet interface to always use slower 10 Mbps speed instead of auto-negotiating an appropriate speed. This is an advanced option intended for networks with special requirements. Do not enable this unless required, as it is much slower than standard auto-negotiated speeds.

**STUN (advanced)**

- Server/Port – Enter your STUN server here. STUN servers may be required to operate with a public SIP server from behind a NAT or router. If using a STUN server, make sure to select the appropriate settings on the Accounts page under SIP Account / Topology.

**RTP**

- Port Range – Select the UDP port range to use for sending RTP audio network traffic during a call. Default range is 23456-23556.
The **System** page configures settings for the access control intercom’s operating system and other administrative functions.
Authentication

- Username – Set the username and password used on the configuration webpages and Telnet shell. Default username and password are “admin” and “admin”.

Syslog

- Report to server - Configures a syslog server that can receive system logs from the access control intercom. This requires a PC or server running a syslog server to receive and store the logs.

Date & Time

- NTP Enabled – Automatically determines the time of day using an NTP server. This is recommended, as the access control intercom does not have a battery-backed clock.

- Server – Enter NTP server address here. The default server is 0.wahsega.pool.ntp.org.

- Daylight saving time – Select this only if daylight saving time is currently in effect in your location.

- Time zone – Select the region that most closely matches your time zone. (Note that daylight saving time is not automatically applied based on region.)
System description

- System contact – The textual identification of the contact / IT person for this device, together with information on how to contact this person. This setting is also available through SNMP as sysContact (1.3.6.1.2.1.1.4), as defined by RFC 1213.

- System name – An administratively-assigned name for this device. By SNMP convention, this is the device’s fully-qualified domain name. This setting is also available through SNMP as sysName (1.3.6.1.2.1.1.5), as defined by RFC 1213.

- System location – The physical location of this device (e.g., “telephone closet, 3rd floor”). This setting is also available through SNMP as sysLocation (1.3.6.1.2.1.1.6), as defined by RFC 1213.
Firmware Management

The Management page has functions for managing the access control intercom’s configuration and firmware.

**Configuration**

- **Backup/Download** – Use this to retrieve a copy of the access control intercom’s current configuration and save to disk.

- **Restore/Upload** – Use this to upload a valid configuration file (file type .JSON) that was retrieved and saved from an access control intercom. *Note that a reboot will be required before the settings take effect.*
Firmware

- Use this to upload new firmware. Firmware updates are available at [www.wahsega.com/resources/downloads](http://www.wahsega.com/resources/downloads) and may only be loaded as .bin file types.

- If your device’s firmware is a version below 2.0.0, you will *first* need to load version 2.0.0.20160531, reboot your device, and *then* load the most current firmware version.

- If your device’s current firmware is version 2.0.0 or above, you may load the most current firmware without any additional steps.

*DO NOT UNPLUG THE ACCESS CONTROL INTERCOM OR INTERRUPT THE FIRMWARE UPGRADE PROCESS BEFORE IT COMPLETES, OR IT MAY BE RENDERED UNUSABLE.*
Appendix A
Making Peer-to-Peer Calls

Peer-to-peer (P2P) calls are SIP calls in which one or both endpoints are not using a centralized SIP server. The access control intercom supports both sending and receiving peer-to-peer SIP calls. Because peer-to-peer calls do not have a centralized SIP server to contact, a peer-to-peer SIP call must always include the network destination in the number called. When sending a call to a peer-to-peer device, the destination is the peer-to-peer device’s IP address or hostname. When placing calls from a peer-to-peer device, the destination could be the IP address or hostname of another peer-to-peer device or the address of a SIP server.

A peer-to-peer SIP address looks like 123@123.456.78.9 or less commonly, 123@peer-to-peer-device.wahsega.com. The username/number comes first, and the IP address or hostname of either the peer-to-peer device or the SIP server comes last.

Setting up Account Information

Note that it is possible for only one phone or endpoint to be in peer-to-peer mode, while the other phone continues to use a centralized SIP server. Thus, the access control intercom must not be in peer-to-peer mode to receive peer-to-peer calls; it can be configured to use a SIP server and still receive peer-to-peer calls. Similarly, the access control intercom can place calls to a peer-to-peer device even if the access control intercom is registered with a SIP server. In both cases, the peer-to-peer call will be routed by the SIP server to/from the access control intercom.

To enable peer-to-peer mode on the access control intercom from the configuration webpages, go to the Accounts page. For the desired SIP account, uncheck the Use SIP server checkbox to put that account in peer-to-peer mode. The Domain checkbox has no meaning in peer-to-peer mode and should be left blank.
Receiving Peer-to-Peer Calls to an Access Control Intercom

If the access control intercom is in peer-to-peer mode, then regardless of how the other phone is configured, place a call to the access control intercom’s username/number @ the access control intercom’s IP address. (For instance, if the access control intercom’s username/number is “123” and its IP address is “123.456.78.9,” place a call to 123@123.456.78.9.)

If the access control intercom is configured with a SIP server and the phone you’re calling from is in peer-to-peer mode, then place a call to the access control intercom’s username/number @ the hostname of the SIP server that the access control intercom is registered on. (For instance, if the access control intercom’s number is “123” and it’s registered on “sip.wahsega.com,” place a call to 123@sip.wahsega.com.)

Placing Peer-to-Peer Calls from an Access Control Intercom

In this instance, it does not matter whether the access control intercom is in peer-to-peer mode or not.

To configure outgoing numbers from the configuration webpages, go to the Lights/Buttons page. For the Phone Number, enter the full destination, containing the destination username/number and IP address (for example, 123@123.456.78.9).
Placing Peer-to-Peer Access Control Intercom Calls on a SIP Server

Even if the access control intercom is in peer-to-peer mode, it can still place calls to a SIP server by explicitly providing the hostname of the SIP server.

For instance, to place a call to username/number “123” on the SIP server sip.wahsega.com, normally it would be sufficient to call 123. From an access control intercom configured in peer-to-peer mode, you can do this by placing a call to 123@sip.wahsega.com, explicitly providing the hostname of the SIP server.
SIP Access Control Intercom with Relay

WL-IC-BKMT-SIP-OV-R
WL-IC-BKMT-SIP-OVNB-R
WL-IC-BKMT-SIP-OV2B-R
WL-IC-FLMT-SIP-I-W-R
WL-IC-FLMT-SIP-INB-W-R
WL-IC-FLMT-SIP-I2B-W-R

User’s Guide
Rev 091416